#8
nLW
2-28-02

Practitioner's Docket No. 2308/102 ***PATENT***

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Sunstein, Bruce D. ; Shapiro, Eileen, C.

Application No.: 09/448,722	Group No.: 2766
Filed: 11/24/1999	Examiner: Not assigned yet

For: Apparatus and Method for Authenticated Multi-User Personal Information Database

Commissioner for Patents
Washington, D.C. 20231
ATTENTION: Group Director, Group 2766 (M.P.E.P., Section 1002.02(c))

PETITION TO MAKE SPECIAL FOR NEW APPLICATION UNDER M.P.E.P. section 708.02, VIII

1. Petition

Applicant hereby petitions to make this new application, which has not received any examination by the Examiner, special.

2. Claims

All the claims in this case are directed to a single invention.

However, if the Office determines that all the claims presented are not obviously directed to a single invention, Applicant will make an election without traverse as a prerequisite to the grant of special status.

3. Search

A pre-examination search was made by the attorney. The field of the search included a DIALOG database search, using terms that included "biometric," "personal data," "personal information," "patient data," "patient information," "emergency data," and "emergency information," in DIALOG files 621 (New Product Announcements) and 275 (Computer Database).

4. Copy of references

There is submitted herewith a copy of the references deemed most closely related to the subject matter encompassed by the claims.

Also attached is Form PTO-1449. (PTO/SB/08A and 08B)

5. Detailed discussion of the references

There is submitted herewith a detailed discussion of the references, which discussion particularly points out how the claimed subject matter is distinguishable over the references.

Also attached is an Information Disclosure Statement.

6. Fee

The fee required by 37 C.F.R. 1.17(i) is to be paid by the attached check for $130.00

Date: January 24, 2002

Keith J. Wood
Registration No. 45,235
Bromberg & Sunstein LLP
125 Summer Street
Boston, MA 02110-1618
US
617-443-9292
Customer No. 2101

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Sunstein et al.
Serial No.: 09/448,722
Date Filed: November 24, 1999
Invention: APPARATUS AND METHOD
FOR AUTHENTICATED MULTI-USER
PERSONAL INFORMATION DATABASE

Att'y Docket: 2308/102
Art Unit: 2766
Examiner: Not yet assigned
Date: January 24, 2002

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patents, Washington, D.C. 20231 on January 24, 2002.

Keith J. Wood
Reg. No. 45,235

Commissioner for Patents
Washington, D.C. 20231

DETAILED DISCUSSION OF THE MOST CLOSELY RELATED REFERENCES

Dear Sir:

The present independent claims require using a set of physiological identifiers to maintain the authenticity of a stored data set, by requiring a comparison of such identifiers whenever the stored data set is modified. The stored data set includes a user's personal information and a representation of the physiological identifiers associated with such user. See, for example, element (d) of claim 1; the second element of claim 17; the terminal portion of claim 29; and element (a)(ii) of claim 31.

As discussed in further detail below, none of the references of record discloses or suggests this limitation.

U.S. Patent No. 5,613,012 of Hoffman et al. (Ref. AA); U.S. Patent No. 5,805,719 of Pare, Jr. et al. (Ref. AB), and U.S. Patent No. 5,838,812 of Pare Jr. et al. (Ref. AC) (hereafter, the "SmartTouch References") disclose a tokenless identification system for authorizing transactions. In order to authorize a transaction, the system of the SmartTouch References compares a biometrics sample (such as a fingerprint or voice recording), gathered from an unknown user, with a previously obtained biometrics sample of the same type. A personal identification code may also be used for authorizing the transaction, in addition to a biometrics sample. In one embodiment, the host system is positioned in series between the individual being identified and other computer networks that are to be accessed (such as the VISANET network and other networks), thereby acting as an interface.

While the SmartTouch References disclose using a biometrics sample for authorizing *transactions*, they do not disclose or suggest using a set of physiological identifiers for gating permission to subjects to *modify* information in a *stored data set itself*, where the stored data set includes a user's personal information and a representation of the physiological identifiers associated with such user. By contrast, the SmartTouch References disclose using biometric samples only to authorize transactions.

The independent claims of the present application therefore differ from the techniques disclosed or suggested by the SmartTouch References.

For example, one embodiment according to the present invention provides a central database of personal information, the authenticity of which is maintained by requiring comparisons of physiological identifiers whenever the personal information is modified. See Application, pg. 9, lines 23-31 and pg. 10, lines 1-10.

Gunnerson, Gary, PC Magazine, February 23, 1999, "Are you Ready for Biometrics?" (Ref. AD) discloses various biometric security devices, such as fingerprint scanners, voice authentication systems, and face recognition systems. However, this reference does not disclose or suggest the use of such systems for maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

PR Newswire, "Iriscan and Anonymous Data Corporation to Develop Medical Records Security System," http://www.iriscan.com, September, 1998 (Ref. AE) discloses a medical records security system in which access to information contained in medical records is secured using a biometric iris recognition system. Throughout a medical testing process, participants have the option to remain anonymous, using only scanned data from their iris as a means of identification. Subsequently, only the individual who owns the test results can access the data, using the iris recognition system. The reference also discloses voluntary sharing of medical data over the Internet, by requiring an individual to provide his biometric code in order to share his test results over the Internet.

This reference does disclose use of a biometric comparison for access to medical information, and for sharing medical information over the Internet. However, it does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

PR Newswire, "The National Registry Inc. Announces Strategic Alliance to Develop and Market New Security Solution for the Internet," July, 1998 (Ref. AF) discloses a website security system that requires presentation of a biometric credential before granting access to a protected web page; the system may be used to provide security for online transactions, and for downloading data from websites.

This reference does disclose use of a biometric comparison for access to websites and online transactions. However, it does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

PR Newswire, "NRI Introduces Finger-Image-Based Use Authentication Solution for Microsoft's Internet Information Server," http://www.nrid.com/, November, 1997 (Ref. AG) discloses use of a biometric finger image identification system in order to grant access privileges to protected resources over the Internet.

This reference does disclose use of a biometric comparison system for access to protected resources over the Internet. However, it does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

PR Newswire, "NRI Finger Imaging Technology Will Enhance Security and Customer Service for Credit Union Members at Unattended Branch Office," http://www.nrid.com/, July 1996 (Ref. AH) discloses use of a finger-image identification system for authorizing financial transactions at unattended "virtual" branch offices of a financial institution.

This reference does disclose use of a biometric comparison system for authorizing transactions. However, it does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

U.S. Patent No. 5,953,419 of Lohstroh et al. (Ref. AI) discloses a cryptographic file labeling system for supporting secured access by multiple users. The disclosure concerns distributing file decryption keys by way of a file security label.

However, this reference does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

U.S. Patent No. 4,993,068 of Piosenka et al. (Ref. AJ) discloses a personal identification system that identifies users at a remote access control site. Physically immutable identification credentials of a user (such as fingerprint, voice, or facial recognition patterns) are stored on a portable memory device, such as a security card. The remote access control site reads the stored identification credentials from the card, and compares them with physical characteristics that the user inputs to a physical trait input device at the remote access control site. If the comparison results in a match, access is granted, for example to a financial network or to a government facility.

This reference involves using physical traits to grant access to users at a remote access control site. However, it does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

International Application WO 00/00882 of LCI/Smartpen, N.V. (Ref. AK) discloses a system for secure transactions and for authenticating a user based on biometric data. A biometric analyzer device is assembled in a secure environment, and has a secure device identifier and encryption key. The system authenticates the user only if two conditions are both satisfied: 1) there is a match between biometric data that the user inputs to the biometric analyzer device, and reference biometric data for that user; and 2) the biometric analyzer device itself is authenticated based on its secure device identifier.

This reference discloses a system that uses biometric data for authenticating a user, and also uses a secure device identifier to authenticate the biometric analyzer device itself. However, it does not disclose or suggest requiring a biometric comparison to permit modification of data in the underlying database. In particular, it does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

UK Patent Application No. GB 2 181 582 A of Blackwell (Ref. AL) discloses a personal identification device, which may be worn, for example, in an item of jewelry such as a wristwatch. The personal identification device stores information from multiple financial accounts on a single device, and allows access to such accounts only upon provision of an identifier such as a fingerprint or voice print of the user. While this reference does disclose storage on the device of personal information such as the user's medical history, emergency medical requirements, driver's license number, etc., these items are described as being "non-secure" (see page 1, line 102-115, especially 103). Accordingly, it appears that access to the personal information on the device (as opposed to the financial account information) is not secured by a requirement of providing a matching physiological identifier; instead, it is non-securely stored on the device, to enable access by officials or during an emergency (see page 1, lines 102-115).

Thus, this reference also does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

International Application WO 98/52115 of Passlogix, Inc.(Ref. AM) discloses a method for providing a user access to a secure application, in which the user must correctly manipulate the layout of an array of symbols in order to be properly authenticated.

However, this reference does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

"National Identification Cards," by Annie I. Anton, http://www.cc.gatech.edu/computing/SW_Eng/people/Phd/id.html, December 17, 1996 (Ref. AN) summarizes national identification card schemes used in Latin American, European, and African nations, and discusses existing and proposed governmental identification card systems in the United States.

However, this reference does not disclose or suggest a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

In conclusion, applicants also note that there is no disclosure or suggestion in any combination of the above references of a technique of maintaining the integrity of a database by requiring a comparison of physiological identifiers whenever an attempt is made to modify a stored data set that includes personal information and physiological identifiers.

Respectfully submitted,

Keith J. Wood
Registration No. 45,235
Attorney for Applicants
Bromberg & Sunstein LLP
125 Summer Street
Boston, MA 02110-1618
(617) 443-9292

183417

GP/~~2766~~ 2131

Practitioner's Docket No. 2308/102 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Sunstein, Bruce D. ; Shapiro, Eileen C.
Application No.: 09/448,722 Group No.: 2766
Filed: 11/24/1999 Examiner: Not yet assigned
For: Apparatus and Method for Authenticated Multi-User Personal Information Database

Commissioner for Patents
Washington, D.C. 20231

CERTIFICATE OF MAILING UNDER 37 C.F.R. section 1.8(a)

I hereby certify that the attached correspondence comprising:

Petition to Make Special for New Application Under MPEP Section 708.02 VIII
Detailed Discussion of Most Closely Related References
Second Preliminary Amendment
Second Supplemental IDS and references AM and AN
Copies of prior IDS's and references submitted in case

is being deposited with the United States Postal Service, with sufficient postage, as first class mail in an envelope addressed to:

Commissioner for Patents
Washington, D.C. 20231

on Jan. 24, 2002.

Keith J. Wood

KJ Wood

Signature of person mailing paper